TRUSTED® COMPUTING GROUP

SPECIFICATION

TCG PC Client Reference Integrity Manifest Specification

Version 1.4

November 2, 2020

PUBLISHED

Contact: admin@trustedcomputinggroup.org

DISCLAIMERS, NOTICES, AND LICENSE TERMS

CONTENTS

1 Scope and Context

Attester integrity and corresponding attestation evidence are critical to many use cases. DICE [21], TPM [22] and platform specifications [7] were designed to provide information—evidence—helpful for Verifiers to determine the state of a platform—the Attester. To that end the TCG Trusted Attestation Protocol (TAP) Information Model specification [1] was created to outline the information presented by the Attester device to the Verifier. The TCG Reference Integrity Manifest (RIM) Information Model (IM) specification [12] compliments the TAP by providing common information elements used by the Verifier to validate the identity of the RIM's creator and the integrity of the support files used to provide the integrity reference information.

This PC Client RIM specification complies with the RIM Information Model and provides addition requirements for PC Client platforms that adhere to the TCG PC Client Platform Firmware Profile [7]. This specification describes the RIM file formats, RIM storage locations within the PC Client, and provides references for the content of the RIM support files.

The PC Client RIM is limited to the integrity reference information necessary for TPM Quote validation by a Verifier for measurements taken during the Attester's boot cycle. Other integrity processes, such as Integrity Measurement Architecture (IMA) [23] are beyond the scope of this specification.

1.1 Audience

This specification is intended to be used by: firmware developers that create firmware compatible with the PC Client Firmware Profile [7]; Verifier developers who need to know the formatting, structure, and usage guidelines for creating and processing a RIM Bundle; and platform developers that need to understand how to create and distribute RIM Bundles. This specification may also be beneficial to OS developers who manage TPM PCRs 8-15.

1.2 Goals

1. To describe the formatting for the common set information elements described by the TCG Reference Integrity Manifest (RIM) Information Model specification
2. To describe the RIM support files for PC Client platforms as required by the RIM Information Model specification.
3. To define default storage locations for RIM Bundles.

1.3 Relationships to other Documents

1.3.1 TCG Documents

There are many TCG documents that use the terminology of Reference Manifest (RM) and Reference Integrity Manifest (RIM). This specification defines the RIM for PC Client platforms.

1.3.1.1 RIM IM

The Reference Integrity Measurement (RIM) Information Model (IM) specification defines an abstract structure for assembling reference measurements (Assertions) that manufacturers and other supply chain entities assert as expected values. The RIM IM requires that a binding specification (this specification) to define a realization of a RIM information model expressions.

1.3.1.2 TAP

The TCG Trusted Attestation Protocol (TAP) Information Model specification provides the information elements used by Verifiers. Not all of the information is required by every Verifier. The RIM is essential for TAP based attestation [1]. The TAP Information Model provides the reference material needed by the Verifier in order to implement the TAP Information Model. Future versions of the TAP Information Model specification may include gathering RIM information from the Attester.

1.3.1.3 FIM

The PC Client Firmware Integrity Measurement (FIM) specification [11] outlines the basic process for collecting, reporting, and processing (attestation) of PC Client firmware. .

1.3.1.4 Platform Certificate Profile

The TCG Platform Certificate Profile specification [10] contains assertions about trust made by a platform manufacturer. The certificate asserts the platform's security properties and configuration as shipped. The Platform Certificate Profile defines a PlatformConfigurationURI attribute that contains "URI where the reference integrity measurements could be obtained by the verifier". The RIM Information Model specification discusses options for the PlatformConfigurationURI attribute..

1.3.2 Non TCG Documents

1.3.2.1 NISTIR 8060

The National Institute for Standards and Technology Interagency Report (NISTIR) 8060 [3], "Guidelines for the Creation of Interoperable Software Identification (SWID) Tags" is the primary reference for the elements described in this specification. NIST IR 8060 pulls its definitions from ISO-IEC 19770-2 and is accessible on the NIST website. Because this specification is focused on integrity there are further restrictions and additional requirements for the information elements that are above and beyond the guidelines found in NISTIR 8060.

1.3.2.2 ISO-IEC 19770-2 (SWID)

ISO-IEC 19770-2 [4] International Organization for Standardization/International Electrotechnical Commission "Software identification tag" is known as the "SWID Specification" and is the main reference source for NIST IR 8060.

1.3.2.3 XML Signature Syntax and Processing

The XML Signature Syntax and Processing Version 2.0 [8] is an informative W3C Working Group Note that describes XML digital signature processing rules and syntax. XML Signatures provide integrity, message authentication, and/or signer authentication services for data of any type, whether located within the XML that includes the signature or elsewhere.

1.4 Terms and Definitions

Asserter: A supply chain entity, manufacturer, vendor or reseller that produces reference values.

Assertions: Reference values.

Attester: A platform or platform component that provides evidence to a Verifier as to its state.

Base RIM: The Base RIM is a RIM Bundle that provides a verifiable identity of the RIM creator and integrity information of support RIMs. The Base RIM contains a digest of each support RIM. The Base RIM also contains a signature.

GUID: Globally Unique IDentifier that is referenced by ISO 19970-2 and is technically identical to the UUID as specified by RFC 4122 [24].

Reference Integrity Manifest (RIM): A Reference Integrity Manifest contains structures that a Verifier uses to validate expected values (Assertions) against actual values (Evidence).

RIM Binding / Binding Specification: A specification that defines conventions for RIM (and RIM Bundle) formatting, marshalling, serialization, digesting, signing, encryption, realization, location, discovery or storage. And

for describing how the information contained in a RIM Bundle is transmitted between Attesters and Verifiers. For example, a RIM Bundle may be marshalled for conveyance over an IP-based communication protocol or instantiated as a file or collection of files in a file system.

RIM Bundle: A collection of a single Base RIM and one or more Support RIMs. A Bundle is created by a single entity at a single point in time.

RIM Bundle Collection: A collection of RIM Bundles typically consisting of a Primary RIM Bundle and one or more Supplemental RIM Bundles.

RIM Creator: Manufactures, System Integrators, Value Added Resellers, Information Technology (IT) support organizations, or endpoint platform owners that create a RIM instance for an Endpoint platform.

RIM GUID: A GUID created as a reference to a specific RIM Bundle. The RIM GUID can be used to link a RIM Bundle to multiple other RIM Bundles.

Supplemental RIM Bundle: Additional RIM Bundles added to a RIM Bundle Collection.

Support RIM: A support RIM contains assertions about the state or configuration of the device to which the RIM applies (a.k.a., Reference Integrity Measurements).

SWID: Software ID tags as defined by ISO-IEC 19770-2.

SWID Schema: An XML schema that describes the structure of the SWID tag.

TCG Event Log: A log file created by the Core Base of Trust for Measurement (CRTM) that is defined in the TCG PC Client Platform Firmware Profile Specification [7].

TCG Event Log Expected Values: A TCG Event Log file, as defined by the PC Client Firmware Profile Specification [7], that is captured by a RIM creator and used as a RIM support file.

TPM PCR Expected Values: A TPM PCR structure that is saved to a file captured by the Primary RIM creator and used as a RIM support file (see section 3.2.1).

Verifier: A system that analyzes evidence from an Attester to determine the Attester's state.

1.5 Keywords

The key words "MUST," "MUST NOT," "REQUIRED," "SHALL," "SHALL NOT," "SHOULD," "SHOULD NOT," "RECOMMENDED," "MAY," and "OPTIONAL" in this document's normative statements are to be interpreted as described in RFC-2119[2]. Key words for use in RFCs to Indicate Requirement Levels.

1.6 Statement Type

Please note a very important distinction between different sections of text throughout this specification. There are two distinctive kinds of text: informative comment and normative statements. Because most of the text in this specification will be of the kind normative statements, the authors have informally defined it as the default and, as such, have specifically called out text of the kind informative comment. They have done this by flagging the beginning and end of each informative comment and highlighting its text in gray. This means that unless text is specifically marked as of the kind informative comment, it can be considered a kind of normative statements.

EXAMPLE: Start of informative comment

This is the first paragraph of 1–n paragraphs containing text of the kind *informative comment* ...

This is the second paragraph of text of the kind *informative comment* ...

This is the nth paragraph of text of the kind *informative comment* ...

To understand the TCG specification the user must read the specification. (This use of MUST does not require any action).

End of informative comment

2 Background

Start of informative comment

The TCG TPM 2.0 Provisioning Guidance [6] describes a set of Golden Measurements that “represent the expected default values of the integrity measurements which the boot firmware and subsequent code generates and extends into TPM PCRs”. The Provisioning Guidance document further states that Platform Manufacturers should deliver a list of expected integrity measurements of the platform BIOS, firmware, and other binaries they provide “as shipped”. Golden Measurements should be included in boot firmware updates, in order to support a given devices lifecycle.

The TCG PC Client Platform Firmware Profile [7] defines a TCG Event Log that captures hashes of firmware and software, firmware configuration settings, and events that are critical to boot operations of the device that extend into the TPM’s Platform Configuration Registers (PCRs). The TCG Event Log can be used by an Attester to serve as the “PCR Log Values” described in the TAP Model that is sent to the Verifier as part of an attestation request. The Verifier needs Reference information in order to validate the log information being sent by the Attester.

The Verifier is also responsible for validating the Quote information sent by the Attester. The Reference information is critical in terms of creating values that can be used to validate the TPM Quote.

A check of the PCR values from a TPM is necessary to ensure that the firmware and firmware configuration has not been altered during post processing and delivery of the Attester device. Once the Attester owner takes possession of the device, they can elect to create RIM bundles to track modifications made to the configuration of the device, if such modifications are required.

End of informative comment

3 PC Client Reference Integrity Measurement (PCRIM)

Start of informative comment

The TCG RIM Information Model specification describes a RIM Bundle that consists of Base RIM and one or more Support RIM (files). The combination of Base and Support RIM represents a RIM Bundle. There may be many RIM Bundles (referred to a RIM Bundle Collection) depending upon the production cycle of a device and the devices associated distribution model.

A RIM Bundle is used by a Verifier as Reference for the appraisal process. To perform the appraisal process, the Verifier also needs an Event Log and a TPM Quote from an Attester (as described by the TAP). The values from theAttester are appraised against the PCRIM during a verification process.

The PCRIM follows guidance as described by the TCG RIM IM (the information model). The following section assumes familiarity with the RIM IM and provides addition requirements for PC Clients.

End of informative comment

3.1 The PC Client Base RIM

Start of informative comment

The Base RIM for PC clients is instantiated as a File. The File contains elements as defined by the RIM IM with the additions or restrictions as noted in this section.

End of informative comment

3.1.1 Base RIM Format

The format for the Base RIM file for PC Clients SHALL be complaint with the ISO/IEC19770-2 (SWID) specification [4] and follow the guidelines presented by NIST IR 8060 (the SWID guidance specification).

3.1.2 RIM Information Model Elements

This specification uses the definitions from Table 1 of the Reference Integrity Information Model specification with the following adjustments:

Element	Attribute	Required	Notes
SoftwareIdentity	tagId	Yes	MUST be a GUID that is the same as the ReferenceManifestGuid created for the TCG Event Log's TCG_Sp800-155-PlatformId_Event field (refer to the TCG PC Client Platform Firmware Profile specification [7] for the definition of the TCG_Sp800-155-PlatformId_Event. The tagID MUST meet the requirements specified by RFC 4122[13]
	Version	Yes	MUST be set to the BIOS version
Meta	BindingSpec	Yes	MUST be a String set to "PC Client RIM". "PC Client RIM" indicates that the RIM Bundle complies with the TCG PC Client RIM Binding specification (this specification)
	BindingSpecVersion	Yes	MUST be in the form of X.Y where X is the major and Y is the minor revision of this specification
	pcURIGlobal	Yes	SHALL be a URI equivalent to the URI found in the platformConfigURI attribute within the Attester's Platform certificate. The platformConfigURI attribute is defined in the TCG Platform Certificate Profile specification [10] and referenced in the TCG Firmware Integrity Measurement [11]
	pcURILocal	Yes	SHOULD be set if the tagCreator stores the RIM bundle on the device
	PayloadType	Yes	SHALL be set to "Indirect"
	supportRIMFormat	Yes	As specified in section 3.2
Payload	supportRIMURIGlobal	Optional	MAY be set to a URI to retrieve a copy of the Support RIM

Table 1: Changes to the RIM IM information elements

3.1.3 Base RIM Signatures

All RIMs SHALL be digitally signed in compliance with W3C XML Signature Syntax and Processing Version 1.1 [8] with the following requirements:

1. The Base RIM MUST use the **Enveloped** signature.
    - **a.** The **KeyInfoReference** element (that provides details on where to get the information to validate the signature) MUST be populated. **KeyInfoReference** MUST use either **KeyName** or the **X509Data** element.
    - **b.** If the **KeyName** is used then **KeyName** SHOULD be set to the subjectKeyIdentifier of the signing certificate**.**
    - c. If the **X509Data** sub element is used to hold a signing certificate then a corresponding Link element MAY exist with a rel attribute set to "signing certificate". The corresponding href value SHALL be set to "embedded". Self signed certificates MUST NOT be used in this field.
2. The Base RIM SHALL use a TCG listed algorithm as a **hashAlgorithm**.
3. The Base RIM SHALL use a TCG listed algorithm as a **sigAlgorithm**.

3.1.4 Base RIM signing certificates

Start of informative comment

The signer of the Base RIM needs to make the set of Certificates (aka the “Certificate path”) used to validate the Base RIM accessible to Verifiers.

End of informative comment

1. Signing Certificates SHALL use TCG listed algorithms.
2. The Authority Information Access (AIA) extension SHOULD be used to define the location of all of the issuer certificates and the URI of the Online Certificate Status Protocol (OCSP) [20] responder (if supported by the Issuer’s Certificate Authority).
3. The Validity period of the Issuing certificates SHOULD be longer than the expected service life of the device.

3.2 PC Client Support RIM

Start of informative comment

The Support RIM concept allows for multiple types of support RIM as specified by the supportRIMFormat attribute. This concept enables new formats to be defined in future versions of this specification. The current set of support RIM formats are by no means a comprehensive set of measurements possible for a specific device. Rather they are a snapshot of values as collected within the Event Logs or PCR values taken at the time of the production or modification of the equipment .

There are currently two formats defined for a PC Client support RIM: TPM PCR Assertion and the TCG Event Log Assertions. The supportRimFormat attribute within the File attribute of the Payload element is used to determine the format being used for the support RIM,

The following section defines the currently defined support RIM formats and how the Support RIM are identified. Support RIM generation is outside the scope of this specification.

End of informative comment

The PC Client RIM Bundle:

1. MUST contain at least 1 Support RIM file.
2. MUST use the supportRimFormat attribute within the Payload File element within the Base RIM to note the support format(s) being specified.

3.2.1 TPM PCR Assertions

Start of informative comment

TPM PCR Assertions are optional for those RIM Bundle creators that cannot utilize the Event Log Assertions due to device limitations or other restrictive conditions. TPM PCR Assertions lacks the detail provided by the Event Log Assertion that is useful for diagnostic purposes. When possible, the Event Log Assertion is recommended to be used.

TPM PCR Assertions that are created by the Platform creator should include at least PCRs 0-7 if the Platform Manufacturer does not include an Operating System. The Platform Manufacturer may include other PCRs as appropriate.

TPM PCR Assertions that are created by entities other than the Platform creator (e.g. the Value Added Reseller) should include all PCRs that were changed from the Platform Manufacturer. The VAR may, however, include all PCRs.

One illustrative example is a Platform Manufacturer that installs firmware but not an Operating system. If the Platform Manufacturer is utilizing the TPM PCR Assertion support RIM then only PCRs 0-7 are included in the TPM PCR Assertion. If a Value Added Reseller adds a NIC card that only changes the value for PCR 2, and no other PCR values are affected, then the VAR should create a supplemental RIM Bundle that contains at least the new value for PCR 2. If the VAR installs an Operating System, the PCR 8-15 should be included as well.

End of informative comment

1. If the TPM PCR Assertions is used then the supportRimFormat attribute within the Base RIM SHALL be set to ”TPM_PCR_Assertions”.

2. TPM PCR Assertions MUST utilize the data from the output of the TPM2_PCR_Read command as defined in the Trusted Platform Module Library Part 3 [19]. The data is equivalent to TPM 2.0 PCR Values defined in the TCG Trusted Attestation Protocol (TAP) Information Model specification. According to the Trusted Platform Module Library Part 3 this information contains:

Type	Name	Description
UINT32	pcrUpdateCounter	The current value of the PCR update counter
TPML_PCR_SELECTION	pcrSelectionOut	The PCR in the returned list
TPML_DIGEST	pcrValues	The contents of the PCR indicated in pcrSelect as tagged digests

Table 2: TPM2_PCR_Read command output

3. The TPM PCR Assertion for a primary RIM Bundle MUST contain (at a minimum) values for the first seven PCRs (PCR 0-7). As an example, a Platform Manufacturer that does not install an Operating System would create a Supplement RIM of type TPM PCR Assertion that includes only PCRs 0-7.
4. The TPM PCR Assertions MUST include all supported TPM hash algorithms supported by the platform firmware and the TPM.

The System Integrator, or Value Added Reseller that adds an OS should create a RIM Bundles that include new support RIM covering PCRs 8-15 at a minimum.

3.2.2 TCG Event Log Assertions

The TCG Event Log Assertions uses a supportRimFormat attribute set to ”TCG_EventLog_Assertion”.

The TCG Event Log Assertion Support RIM is a binary file (no formatting) containing the Events captured by the S-CRTM as specified by the PC Client Platform Firmware Profile [7]. An example of the event log can be found in Appendix A: PC Client Base RIM Example.

3.3 EFI System Partition Storage

Start of informative comment

Storage for the PC Client RIM Bundles is defined in this section as convenience for the end user. OEMs, System Integrator, and Value Added Resellers should use the platformConfigURI attribute within the Platform Certificate in order to provide a flexible, agile, and security centered approach for Verifiers to obtain RIM Bundles.

End of informative comment

The Primary RIM Creator (the entity that creates the initial RIM Bundle) SHALL place the RIM Bundle on the Attester device within a tcg/manifest directory located on the EFI System Partition (ESP). Per the SWID guidance document [3] a subdirectory named “swidtag” is used to hold the Base RIM file. Another subdirectory of the tcg directory named “rim” holds the RIM support files. The directories used by a PC Client for storing RIM files SHALL be:

Directory	Files
/boot/tcg/manifest/swidtag	Base RIM Files
/boot/tcg/manifest/rim	Support RIM Files

Table 3: Directory Structure for RIM Files

3.3.1 File naming conventions

Start of informative comment

Since there can be multiple organizations creating RIM Bundles for a given device a naming convention is required ensure the uniqueness of each RIM file.

End of informative comment

3.3.1.1 The Base RIM file name

Per the NISTIR 8060 SWID guidance document [3] the following naming convention SHALL be used:

For the Base RIM file:

<name of the tag creator> + <product name> + <RIM version>.swidtag

Where:

1. “name of the tag creator” is the “name” attribute of the Entity element defined in the RIM Information Model specification
2. “product name” is the “name” attribute of the SoftwareIdentity element defined in the RIM Information Model specification.
3. “RIM version” is the “version” attribute of the SoftwareIdentity element defined in the RIM Information Model specification . Note that version attribute is set to BIOS version as specified in section 3.1.2.

Example: acme.com.BigProduct.3.swidtag

3.3.2 RIM Support File names

The TCG Event Log Assertions files SHALL use the following naming convention:

<name of the tag creator> + <product name> + <product version>.rimel

The TPM PCR Assertions files SHALL use the following naming convention:

<name of the tag creator> + <product name> + <product version>.rimpcr

Examples:

acme.com.BigProduct.3.rimel

acme.com. BigProduct.3.rimpcr

4 RIM Lifecycle

Start of informative comment

The RIM Information Model specification describes a lifecycle that allows for multiple organizations to participate in the production, distribution, and maintenance of the Attester Device. For PC Clients the RIM Bundle is inherently bound to the Firmware lifecycle. The RIM Bundle should be updated during the process of updating the Firmware. .

End of informative comment

4.1 RIM Bundle Creation

Start of informative comment

The Primary RIM Bundle is installed by the Platform Supplier (the tagCreator). The RIM Bundle is installed in the EFI partition in accordance with section 3.3.

End of informative comment

4.2 Pre Delivery RIM Bundles

Start of informative comment

When a System Integrator or Value Added Reseller make modifications that require a new RIM Bundle, the RIM Bundle is installed in the EFI partition in accordance with section 3.3 **Error! Reference source not found.** The RIM Bundle is considered "supplemental" to the Primary RIM Bundle created by the Attester Device Manufacturer.

End of informative comment

4.2.1 Supplemental RIM Bundles

Start of informative comment

The RIM Information Model specification allows for pre-delivery modifications by System Integrator and Value Added Resellers as well as post-delivery modifications by IT organizations. A modification will require the creation of a supplemental RIM Bundle if the modification changes any reference value contained within the existing RIM Bundle collection. Examples of modifications that require a new RIM Bundle will include:

- Firmware updates that occurred after the device has completed the production cycle.
- Modification of a system component that contains Option ROMs (e.g. NIC or Graphic cards).
- Installation of an Operating System.
- Installation of an EFI user application (e.g. system diagnostic applications).
- Modification of the firmware configuration that may change measured settings (e.g. boot order, secure boot enable, etc.).

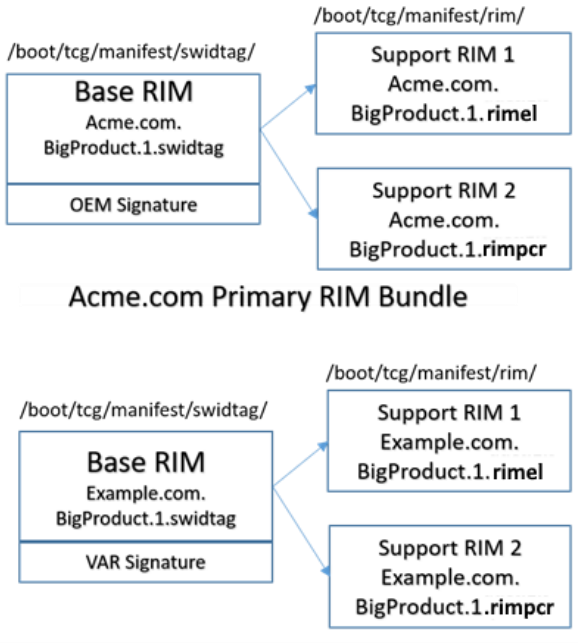

Figure 1 RIM Bundle Collection with Bundle added by a VAR

As discussed in the RIM information Model specification, , the VAR sets the VAR specific information in the entity element of the Base RIM. The VAR also needs to provide either a TCG Event Log Assertions or a TPM PCR Assertions File(s) along with payload file hashes placed in the Base RIM file. Each VAR should only create a single RIM Bundle.

End of informative comment

The System integrator or Value Added Reseller can make a supplemental RIM Bundle that provides a new set of RIM files as illustrated in figure 2:

1. Supplemental RIM bundles SHALL have the supplemental attribute within the Base RIMs SoftwareIdentity element be set to “true”.
2. The Rim Bundle file names are unique and should not conflict with the Primary RIM Bundle.
   The System Integrator or Value Added Reseller SHALL NOT remove any RIM Bundle as the information in the other RIM Bundles may provide valuable information in an investigation attempting to track down unauthorized modification detected by a Verifier.

As an example, the following illustrates a Linux based directory structure after the example in this section is completed:

```
/boot/tcg/manifest/
                |--- /rim/
                      | -- Acme.com.BigProduct.1.rimel
                      | -- Acme.com.BigProduct.1.rimpcr
                      | -- Example.com.BigProduct.1.rimel
                      | -- Example.com.BigProduct.1.rimpcr
                |--swidtag/
                      | -- Acme.com.BigProduct.1.swidtag
                      | -- Example.com.BigProduct.1.swidtag
```

4.3 Supply Chain Processing using the RIM

Start of informative comment

An organization procuring a new device (an Attester Device owner or designated Maintenance Organization) that applies this specification may choose to use the RIM as a means of verifying the Firmware and Boot Manager installed on the device. This process involves the use of a Verifier to perform either the PCR Composite or Event Log Verification. Part of the process involves the transfer of all RIMs on the devices to the Verifier. The Verifier is responsible for obtaining the Trust Anchors/Certificate paths used for validating the signatures on the RIMs prior to performing the validation.

End of informative comment

4.3.1 Optional Reimaging

Start of informative comment

Some organizations may choose to reimage the device for security or maintenance reasons. This generally involves using an OS specific installer that will remove any existing OS and install an approved OS (not necessarily the newest available version) as well as performing some initial configuration and setup the device needs to meet local organizational policies and guidelines. This may invalidate some or all of the RIM Bundle Collection(s). The re-imaging may also (optionally) include reflashing the firmware to a known revision. If the organization chooses to perform PCR Composite Event Log Verification after re-imaging then the guidance for this case is:

1. Back up the RIM delivered with the device as it may be destroyed when the device is re-imaged.
2. Create a new RIM when the device is re-imaged. This includes signing the RIM with a signing key that has an Organization-approved Certificate.
3. Verify that the new RIM Bundle contains correct measurements for each device using an OEM provided, commercially available, or open source tool (if available). These tools may require the RIM Bundle as a prerequisite or require internet access to obtain RIM Bundles associated with the newly installed OS and or firmware.
4. Import the new RIMs into the Verifier for future verifications.

End of informative comment

4.4 Maintenance updates

Start of informative comment

As described in the RIM Information Model, an IT Organization (an Attester Device owner or designated Maintenance Organization) may decide to manage configuration changes by creating RIM Bundles. The new RIM Bundle is considered a supplemental RIM and follows section 4.2.1. Refer to the Maintenance update section (section 5.3) of the TCG Reference Integrity Manifest (RIM) Information Model specification for further details.

End of informative comment

4.5 Firmware Updates

Start of informative comment

Firmware updates require an updated RIM to be created by the Platform Manufacturer (or delegated representative). The updated RIM should follow the guidance given in the TCG Reference Integrity Manifest (RIM) Information Model specification section 5.4.

End of informative comment

Appendix A: PC Client Base RIM Example

The following example uses an 2048 bit RSA key pair with an associated Self signed certificate representing the Example.com corporation. The following parameters will be used:

Software Identity Name: Example.com BIOS
 version : 01
 tagId: 94f6b457-9ac9-4d35-9b3f-78804173b65as
 tagVersion:0
Entity (tagCreator) Name
 Regid: http://Example.com
 Role: softwareCreator tagCreator
Links:
 installation media url: https://Example.com/support/ProductA/firmware/installfiles
Meta:
 colloquialVersion: Firmware_2019
 Edition: 12
 Product: ProductA
 Revision: r2
 PayloadType: Indirect
 PlatformManufacturerStr: Example.com
 PlatformManufacturerId: 00201234
 PlatformModel: ProductA
 PlatformVersion:01
 FirmwareManufacturerStr: BIOSVendorA
 FirmwareManufacturerId: 00213022
 FirmwareModel:A0
 FirmwareVersion: 12
 BindingSpec: PC Client RIM
 BindingSpecVersion: 1.2
Payload:
 Directory: /boot/tcg/manifest/swidtag
 File1: Example.com.iotBase.bin
 Version: 01.00
 size= 15400

Key used for the example:

An RSA 2048 bit key will be used as the key for signing the Base RIM. Keys and certificate will be shown in PEM format. The TCG Log will be show in base 64 encoding.

Private Key (RSA 2048 bit private key – no password):

-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAp3WVYaRJG7EABjbAdqDYZXFSTV1nHY9Ol9A5+W8t5xwBXBry
ZCGWxERGr5AryKWPxd+qzjj+cFpxxkM6N18jEhQIx/CEZePEJqpluBO5w2wTEOe7
hqtMatqgDDMeDRxUuIpP8LGP00vh1wyDFFew90d9dvT3bcLvFh3a3ap9bTm6aBqP
up5CXpzrwIU2wZfgkDytYVBm+8bHkMaUrgpNyM+5BAg2zl/Fqw0qotjaGr7PzbH+
urCvaGbKLMPoWkVLIgAE8Qw98HTfoYSFHC7VYQySrzIinaOBFSgViR72kHemH2lW
jDQeHiY0VIoPik/jVVIpjWe6zzeZ2S66Q/LmjQIDAQABAoIBAHJxvJ6XfVNMexzE
DHLGaD2j3cB7xf4As5CzQPvETNW2YQOGcwOVpQkLNFfFqvacl45+1qfLcbBtT3ZU
+ZNgFILFaF7kdEeCCsr2B0BvUrRIxxr1lEZsCXS5Z0oPIUmKhCf+drWjVAzuvjCP
H4ImkA3fMNK8heDgqS8vRiXZ35BmGQMnpm91EhVHY/0uuzVasZ7wHxTDORapChoZ
KMu8AUYDunjnib6E6vCzIj4qaJ8MBQ1uNPWUrW65NX9TrM7Lf1LxVFgPQXQ33qD5
hUetct3gec5TEBvDIa9r+Yb5I/Uz1xVOBZuBM2dYf+tHHVqD+l2Aj+xdjamfDfLu
FAUDQCECgYEA3BiMORiRL0RfhRU00YWGrTEZ/NAxk1Y3U99jIGo3SsdOTlsQZkLB
aG9+H4kp69MAFzyXg1xuK7jARNm0pBAvKwjtPBvIoUKB/MdHL7hEXtX6VVpN0Vjb
nFRiIiUhFwCMFq5WGS032HeRqgZDxDkMcaODLTsqnh5lR9ZjssJPQAUCgYEAwsbf
eZbs6kGVfV5e/EELziG4znRy42Nt2cqfLBrfW4qy/1md90wkYJh9XutQXa0qjuzp
v2opdmOfVzOVFOpC2w49ClJjj07KySZiFX/K92ypbVVGi3j4K+Mnse3ZrR0R/DpC
1ypxNEQjtJAovZCTAddshN6VsZPj7s87UHd2uukCgYATSXdoPXXjjXtNXzlcrvXJ
UYc0d04Q2jpI+EdofMZRoDuFdEdwnqLyMur7enqY9smIP8ALO9tPq4X1wpoo0l4/
yC152flv4DMh4pijXuNm6BtixWISWVYNUfuzgEtxB5Q/HJHg7Ox65Kd4HcpsdI9Z
mfmRyiCG8KTxcaEU9iAZvQKBgQCNGWyCtKbj/KbCrz64FpbquNscFJe1yi2l/Hba
iI0Nz6hj+xPINkyT/WO1A1qwweV2rIGYvNtUfE7N6PwyrpHIBsSICYz+H+IfXcLo
OC9clkcWgRQdrYB6qo/zAY8TLV/+DGanYIOpjUMgZt5clQMp7lka1/QxNCWGtnEN
lb1ZIQKBgQDAb/6E/Nd8NNO+fT5pDlMb9y10ybmAW6tEZoGtuYzd6MPC6xkHUlYO
xf2n9yOSlBe5i4noA8taZEX2rslx+/loRKp3/Orw68z6crQzMYp1jkGbrAqnlh2/
p7lU7i9xb/hsRHcFRmCP+5RSewf/4T+a1Pd2aGGO7FnBlammhJDEVA==
-----END RSA PRIVATE KEY-----

X509 Certificate holding the public portion of signing key used for validating the signature of the RIM :

-----BEGIN CERTIFICATE-----
MIIDoTCCAomgAwIBAgIJAPB+r6VBhBn5MA0GCSqGSIb3DQEBCwUAMFMxCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJWQTEQMA4GA1UECgwHRXhhbXBsZTERMA8GA1UECwwI
UENDbGllbnQxEjAQBgNVBAMMCUV4YW1wbGVDQTAeFw0yMDAzMTExODExMjJaFw0z
MDAxMTgxODExMjJaMFwxCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJWQTEQMA4GA1UE
CgwHRXhhbXBsZTERMA8GA1UECwwIUENDbGllbnQxGzAZBgNVBAMMEmV4YW1wbGUu
UklNLnNpZ25lcjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKd1lWGk
SRuxAAY2wHag2GVxUk1dZx2PTpfQOflvLeccAVwa8mQhlsRERq+QK8ilj8Xfqs44
/nBaccZDOjdfIxIUCMfwhGXjxCaqZbgTucNsExDnu4arTGraoAwzHg0cVLiKT/Cx
j9NL4dcMgxRXsPdHfXb0923C7xYd2t2qfW05umgaj7qeQl6c68CFNsGX4JA8rWFQ
ZvvGx5DGlK4KTcjPuQQINs5fxasNKqLY2hq+z82x/rqwr2hmyizD6FpFSyIABPEM
PfB036GEhRwu1WEMkq8yIp2jgRUoFYke9pB3ph9pVow0Hh4mNFSKD4pP41VSKY1n
us83mdkuukPy5o0CAwEAAaNvMG0wHQYDVR0OBBYEFC/euOfQMKIgnaoBhhqWT+3s
8rzBMB8GA1UdIwQYMBaAFEahuO3bpnFf0NLneoo8XW6aw5Y4MAkGA1UdEwQCMAAw
CwYDVR0PBAQDAgbAMBMGA1UdJQQMMAoGCCsGAQUFBwMDMA0GCSqGSIb3DQEBCwUA
A4IBAQBl2Bu9xpnHCCeeebjx+ILQXJXBd6q5+NQlV3zzBrf0bleZRtsOmsuFvWQo
KQxsfZuk7QcSvVd/1v8mqwJ0PwbFKQmrhIPWP+iowiBNqpG5PH9YxhpHQ1osOfib
NLOXMhudIQRY0yAgqQf+MOlXYa0stX8gkgftVBDRutuMKyOTf4a6d8TUcbG2Rnyz
O/6S9bq4cPDYLqWRBM+aGN8e00UWTKpBl6/1EU8wkJA6WdllK2e8mVkXUPWYyHTZ
0qQnrYiuLr36ycAznABDzEAoj4tMZbjIAfuscty6Ggzxl1WbyZLI6YzyXALwaYvr
crTLeyFynlKxuCfDnr1SAHDM65BY
-----END CERTIFICATE-----

X509 Example.com CA Certificate used to validate the Certificate Path of the Certificate:

-----BEGIN CERTIFICATE-----
MIIDjDCCAnSgAwIBAgIJALEA1Q472tZoMA0GCSqGSIb3DQEBCwUAMFMxCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJWQTEQMA4GA1UECgwHRXhhbXBsZTERMA8GA1UECwwI
UENDbGllbnQxEjAQBgNVBAMMCUV4YW1wbGVDQTAeFw0yMDAyMTAxNzI2MDdaFw0y
OTEyMTkxNzI2MDdaMFMxCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJWQTEQMA4GA1UE
CgwHRXhhbXBsZTERMA8GA1UECwwIUENDbGllbnQxEjAQBgNVBAMMCUV4YW1wbGVD
QTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAPN0k+ULqFxdHZ14CCio
HAvn56T1Ca4t3ClmZoHSAiKsqzLV+rErk5SbMTIdi0vHQ+3sPYf9Opy0EeUXzh4J
g6CeGdDn247has1k135KBD9iJCaErJfZPnJ22CjKey8rvJM8fH3CAR7M/5uwYcPH
yRICwGAJMA/Qss4nsMRQpfZg4ReKVW+kAoa9eekG3q1sLu/QlCb0NC766X0ANP+8
AuGuHJmNV22fjvwSNfWbsJElcMrLbK4kliPyy05YVs19p+cBM1ADxGw2fJqsNsUy
34SXL1ATqOp7VCslRR5TJBzhxfM56xZbszry7BaqTSFDRGn1FuMw/4+qtPMAB88u
eXECAwEAAaNjMGEwHQYDVR0OBBYEFEahuO3bpnFf0NLneoo8XW6aw5Y4MB8GA1Ud
IwQYMBaAFEahuO3bpnFf0NLneoo8XW6aw5Y4MA8GA1UdEwEB/wQFMAMBAf8wDgYD
VR0PAQH/BAQDAgGGMA0GCSqGSIb3DQEBCwUAA4IBAQCwCUSV6VjOR+v85z18q5UX
bla0gEsfbc2mx0kGtNqi2im2Xt8UoSJDnfMXzfQq3IP3en943mqgIeYUl3f9UQBT
KgGfyHNbEfa0FzqfKpxJdT37C9ilSQ85GtThffc4I50QgBHaRXOvwBdrGpU2O11V
x35VLyYoyclIg+CizVywEX53aoMil1hEbv0TPtbNnFZGwM/fxvere65GeQld9gEP
9krGtSXYlMktvr66cqPzmG0ciA6dMBZN8dpTgUopmYNz8HVoHDq/KBmXYA7CMzrX
pVNx4kMW/KxA+XAHT82xE7PCiLIJx4z9uPn0O4PBDw0tQ0mxuDpeoi1i9PuBfe6Y
-----END CERTIFICATE----

TCG Event Log used as a Support RIM (Base64 encoded):

AAAAAAMAAAAAAAAAAAAAAAAAAAAAAAAAAACEAAABTcGVjIElEIEV2ZW50MDMAAAAAAAACAAIB
AAAACwAgAAAAAAAACAAAAAEAAAALAJailtIk8oXGe+6Tww+KMJFX8NqjXcW4fkELeGMKCc/HAgAA
AAAAAAAAAgAAIABAAAACwDbx/wtGEXfo/h/5mGnogCieY0b3FWq8PS18un7vKVGaxAAAAAAcCBr
AAAAAAAADQAAAAAAAAAAAgAAIABAAAACwBgzOm9fMIZbpzQWFO+ilZKDIxK7BJBH4mBrvoE6C8g
zxAAAAAwP1qAAAAAACwIgAAAAAAAAAAAgAAIABAAAACwBp9xKEOd/R3EZN88oxOl8uN4NkZZHe
slWjcuXpr+LQ3RAAAAAAAD/AAAAAAAAfwAAAAAAAAAAAgAAIABAAAACwDjsMRCmPwcFJr79MiZ
b7kkJ65B5GSbk0yklZkbeFK4VRAAAAAAAAAAAAAAAAAABAAAAAAAAAAAAEAAAABAAAACwABcqpE
MEaA4ID7o1JobrFSFrwU7IIp8TjrJZGHMuMf9gkAAABBQ1BJIERBVEEAAAAAAQAAAAEAAAALAMW/
KK0NvxyNvKzlV0kc2lldTVDffitzghcMwgMDd1f9CQAAAEFDUEkgREFUQQcAAAABAACAAQAAAAsA
EVqoJ9vM+0TSFq2ez9pWvepiC4YKlL7Vt6J7uhxNAtg1AAAAYd/ki8qT0hGqDQDgmAMrjAoAAAAA
AAAAAQAAAAAAABTAGUAYwB1AHIAZQBCAG8AbwB0AAAHAAAAAQAAgAEAAAALAN6nuAq1Oj2qok1c
xGxk4fqf/QNzn5Cq29jAhnxKW0iQJAAAAGHf5IvKk9IRqg0A4JgDK4wCAAAAAAAAAAAAAAAAAAAA
UABLAAcAAAABAACAAQAAAAsA5nDhIfzr1HO4vEG7gBMB/B2a+jOQTwb3FJt08SxHpo8mAAAAYd/k
i8qT0hGqDQDgmAMrjAMAAAAAAAAAAAAAAAAAAABLAEUASwAHAAAAAQAAgAEAAAALALr4mjzKzlJ1
DF8BKDUeBCKkFZehrf1QgiqjY7nRJOp8JAAAAMuyGdc6PZZFo7za0A5nZW8CAAAAAAAAAAAAAAAA
AAAAZABiAAcAAAABAACAAQAAAAsAn3W2gjv/avECSk4gNnGc3VSNPLwr8d6OfvTQ7QH5S/kmAAAA
y7IZ1zo9lkWjvNrQDmdlbwMAAAAAAAAAAAAAAAAAABkAGIAeAAHAAAABAAAAAEAAAALAN8/YZgE
qS/bQFcZLcQ910jqd4rcUrxJjOgFJMAUuBEZBAAAAAAAAACAAAABAAAgAEAAAALACqvZTY45Dc7
z6s7nUfF5/Uc33B49/AGG+Dy4rzhnDr5TAAAABgg1FgAAAA4LQFAAAAAAAAAAAAAAAACwAAAAA
AAAABAcUACzi7bYw3vpFuwnKICwWVLcEBhQAGuPhFZ2fhEyC+xpwf8D2O3//BAACAAAABAAAgAEA
AAALANObKed0EcnNtq3uu+Nlv1+VgQ2ai+niuRpy79h1vKVsTAAAABgg1FgAAAA4LQFAAAAAAAA
AAAAAAAAACwAAAAAAAABAcUACzi7bYw3vpFuwnKICwWVLcEBhQABSBLtLxCyUGAr6vX3H1pI3//
BAACAAAABAAAgAEAAAALAFnskpveeL99s8R1vpVaQU7jAJ4efewzTq+72WmloOsVTAAAABgg1VgA
AAAAYLYEAAAAAAAAAAAAAAAAAACwAAAAAAAABAcUACzi7bYw3vpFuwnKICwWVLcEBhQA6jb0oSeh
+E6VfIBIYG/2cH//BAACAAAABAAAgAEAAAALAJlj0AGzxTcx+YUPtvEA1nYBy6vRb1RGl+eUzWlO
zUD0TAAAABgw5VgAAAAYBgEAAAAAAAAAAAAAAAAACwAAAAAAAABAcUACzi7bYw3vpFuwnKICwW
VLcEBhQAkhYAXG0GsEW7hZyL32wIRX//BAACAAAABAAAgAEAAAALADnmYNXGbhra/Z3XO7TDnV6A
ima+7/JXZbogVVwnQHyeTAAAABgg5lgAAAAwCwDAAAAAAAAAAAAAAAAACwAAAAAAAABAcUACzi
7bYw3vpFuwnKICwWVLcEBhQA1ead6jl490aeY03osA4uXX//BAACAAAABAAAgAEAAAALAIH5mR7R
98VqMqSkB52GJAtJpiQhpnI/Ac2DueD/3feSTAAAABhA7FgAAAAyCABAAAAAAAAAAAAAAAACwA
AAAAAAAABAcUACzi7bYw3vpFuwnKICwWVLcEBhQAb7ihVkoNXUiH3q0OuhyMKn//BAACAAAABAAA
gAEAAAALAEU3DFfAIxiroBZDIYSRmnAcYP0WQUC8H83fd3PcXRPzTAAAABjQ7FgAAAAIJMAAAAA
AAAAAAAAAAAACwAAAAAAAABAcUACzi7bYw3vpFuwnKICwWVLcEBhQAdq3kgZRqT02iOZP+LE55
sH//BAACAAAABAAAgAEAAAALALWqxVrbB6+w3Y0Nykp5O0pIt1SUi4e5jGsPR7wGSFViTAAAABhw
vVgAAAA4DgDAAAAAAAAAAAAAAAACwAAAAAAAABAcUACzi7bYw3vpFuwnKICwWVLcEBhQAOplB
ZvMsrEyFBlmcsCdqvX//BAACAAAABAAAgAEAAAALAELnKzYQq30uIz3lzqfqANcMIvQJBZKBLUDT
mz6ZgBwITAAAABig5lgAAAAwKIBAAAAAAAAAAAAAAAACwAAAAAAAABAcUACzi7bYw3vpFuwnK
ICwWVLcEBhQALID9nKEJ1kOCF6pJwfkNLH//BAACAAAABAAAgAEAAAALAHrMewaBDx14l+vlY2pF
vNpyHy6xuwBwRkvlSAT67QSSTAAAABhA51gAAAAAAAABAAAAAAAAAAAAAAACwAAAAAAAABAcU
ACzi7bYw3vpFuwnKICwWVLcEBhQAu/sutiM5uUym6NuBjoKKgH//BAACAAAABAAAgAEAAAALAJBU
2rhR+/CAMurPQ2RW3uZvAGRPGH7FMZ2zRR8y6pgSTAAAABjg01cAAAAA4PMEAAAAAAAAAAAAAAAA
ACwAAAAAAAABAcUACzi7bYw3vpFuwnKICwWVLcEBhQAXjLknD4A4xG1grisbxmaV3//BAABAAAA
AgAAgAEAAAALAFw2KCDmPaAAoiFHb8wtUJBB7WrRbp8EDnhpobukUkRqPgAAAGHf5IvKk9IRqg0A
4JgDK4wJAAAAAAAAAwAAAAAAAAAQgBvAG8AdABPAHIAZABlAHIABAADAAIAAAABAAUAAQAAAAIA
AIABAAAACwAAj01F8blYrm5ULjwlAPBO3kxYOFSEDLbirzJsX3cDZFwBAABh3+SLypPSEaoNAOCY
AyuMCAAAAAAAAAAsAQAAAAAAAEIAbwBvAHQAMAAwADAANAABAAAAdABXAGkAbgBkAG8AdwBzACAA
QgBvAG8AdAAgAE0AYQBuAGEAZwBlAHIAAAAEASoAAgAAAACoDwAAAAAACADAAAAAAA8YqeMHgSr
T4wS9JqGuF1zAgIEBEYAXABFAEYASQBcAE0AaQBjAHIAbwBzAG8AZgB0AFwAQgBvAG8AdABcAGIA
bwBvAHQAbQBnAGYAdwAuAGUAZgBpAAAAf/8EAFdJTkRPV1MAAQAAAIgAAAB4AAAAQgBDAEQATwBC

AEoARQBDAFQAPQB7ADkAZABlAGEAOAA2ADIAYwAtADUAYwBkAGQALQA0AGUANwAwAC0AYQBjAGMA
MQAtAGYAMwAyAGIAMwA0ADQAZAA0ADcAOQA1AH0AAABEAAEAAAAQAAAABAAAAH//BAABAAAAAgAA
gAEAAAALAIDiPsAeS6BQW55inBeRUEcSclAGqJLDI0fKek7HlwHvwAAAAGHf5IvKk9IRqg0A4JgD
K4wIAAAAAAAAAJAAAAAAAAAAAQgBvAG8AdAAwADAAMAAzAAEAAAAgAFUARQBGAEkAIABJAE4AVABF
AEwAIABTAFMARABTAEMAMgBCAFcAMgA0ADAAQQA0ACAAQwBWAEQAQQA1ADEANgA1ADAANwA3AFEA
MgA0ADAAMwBHAE4AIAAAAAIBDADQQQMKAAAAAAEBBgAFEQMSCgAAAP//AAB//wQATqwIgRGfWU2F
DuIaUixZsgEAAAACAACAAQAAAAsAKxdJs+Jp/D1Eg9GWAvPCI6nu+XHJbxWp54QdV4QRbw6EAAAA
Yd/ki8qT0hGqDQDgmAMrjAgAAAAAAAAVAAAAAAAAAABCAG8AbwB0ADAAMAAwADIAAQAAACwAQgBv
AG8AdAAgAEQAZQB2AGkAYwBlACAATABpAHMAdAAAAAQHFAA1e7vNM2jWTpqyV9Ks3fbwBAYUANxb
wu7yZ5VNsdX4GyA50R1//wQAAQAAAAIAAIABAAAACwDu939CA4ZXc7inmKR7sTy6AcFqbnXTi2c6
LHKoDlQRmXoAAABh3+SLypPSEaoNAOCYAyuMCAAAAAAAAABKAAAAAAAAAEIAbwBvAHQAMAAwADAA
MAAJAQAALABFAG4AdABlAHIAIABTAGUAdAB1AHAAAAAEBxQANXu7zTNo1k6aslfSrN328AQGFAAh
qixGFHYDRYNuirb0ZiMxf/8EAAEAAAACAACAAQAAAAsALDK8yOC/SEEBxfA8LQpVLGI6Hjf77vXH
jj0/ri4Y8y6KAAAAYd/ki8qT0hGqDQDgmAMrjAgAAAAAAAAWgAAAAAAAABCAG8AbwB0ADAAMAAw
ADEAAQAAACwAVQBFAEYASQAgAEkAbgB0AGUAcgBuAGEAbAAgAFMAaABlAGwAbAAAAAQHFAA1e7vN
M2jWTpqyV9Ks3fbwBAYUAIOlBHw+nhxPrWXgUmjQtNF//wQAAQAAAAIAAIABAAAACwDb2u69L8di
bpWx9aPWu/WkOBRLV7EW8Ko2VCQeh78NIdAAAABh3+SLypPSEaoNAOCYAyuMCAAAAAAAAACgAAAA
AAAAAEIAbwBvAHQAMAAwADAANQABAAAAHABVAEUARgBJACAASwBpAG4AZwBzAHQAbwBuACAARABh
AHQAYQBUAHIAYQB2AGUAbABlAHIAIABHADMAIAAwADAAMQBDAEMAMABFAEMAMwA0AEYAMQBCAEIA
OAAxADkANwAxADcAMAAxADkANQAAAAIBDADQQQMKAAAAAAEBBgAAFAMFBgADAH//BABOrAiBEZ9Z
TYUO4hpSLFmyBAAAAAcAAIABAAAACwA9Z3K0+E7UdZXXKixMX/0V9btyx1B/4m8qruLGnVYzuigA
AABDYWxsaW5nIEVGSSBBcHBsaWNhdGlvbiBmcm9tIEJvb3QgT3B0aW9uAAAAAAQAAAABAAAACwDf
P2GYBKkv20BXGS3EPddI6neK3FK8SYzoBSTAFLgRGQQAAAAAAAAAAQAAAAQAAAABAAAACwDfP2GY
BKkv20BXGS3EPddI6neK3FK8SYzoBSTAFLgRGQQAAAAAAAAAAgAAAAQAAAABAAAACwDfP2GYBKkv
20BXGS3EPddI6neK3FK8SYzoBSTAFLgRGQQAAAAAAAAAAwAAAAQAAAABAAAACwDfP2GYBKkv20BX
GS3EPddI6neK3FK8SYzoBSTAFLgRGQQAAAAAAAAABAAAAAQAAAABAAAACwDfP2GYBKkv20BXGS3E
PddI6neK3FK8SYzoBSTAFLgRGQQAAAAAAAAABQAAAAQAAAABAAAACwDfP2GYBKkv20BXGS3EPddI
6neK3FK8SYzoBSTAFLgRGQQAAAAAAAAABgAAAAQAAAABAAAACwDfP2GYBKkv20BXGS3EPddI6neK
3FK8SYzoBSTAFLgRGQQAAAAAAAAAAQAAAAkAAIABAAAACwA2ZtFsMOvEbKMsfG4yIhdaoVCB3Z0k
tkkzzTP3ZMyauSAAAAABAAAAAAAAAEQV/fKUlyxKmS7lu88g45QAAGdjAAAAAAUAAAAGAACAAQAA
AAsA8Vd8obkDMUXIrE3K3PuvxeFflPo+zpvnROXntEITORPkAgAARUZJIFBBUlQAAAEAXAAAAKBx
MQwAAAAAAQAAAAAAAACvRPIbAAAAACIAAAAAAAAAjkTyGwAAAABv58NOI3k+TLBA6AgPG4iDAgAA
AAAAAACAAAAAgAAAANC+BUkFAAAAAAAAAKS7lN7RBkBNoWq/1QF51qyHh8xCI9tFTpmBcBrcgB3H
AAgAAAAAAD/pw8AAAAAAAEAAAAAAACAQgBhAHMAaQBjACAAZABhAHQAYQAgAHAAYQByAHQAaQB0
AGkAbwBuAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
p4weBKtPjBL0moa4XXMAqA8AAAAAAP/HEgAAAAAAAAAAAAAAAAIBFAEYASQAgAHMAeQBzAHQAZQBt
ACAAcABhAHIAdABpAHQAaQBvAG4AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
XAu4TYF9+S3wAhWu/8+Q2AwyRU+2z6TYvubZywDIEgAAAAAA/8caAAAAAAAAAAAAAAAAAgE0AaQBj
AHIAbwBzAG8AZgB0ACAAcgBlAHMAZQByAHYAZQBkACAAcABhAHIAdABpAHQAaQBvAG4AAAAAAAAA
AAAAAAAAAAAAAKKg0OvluTNEh8BotrcmmcccTCUMEkuISriEQqMYZqNIAMgaAAAAAAD/P/gaAAAA
AAAAAAAAAAAAQgBhAHMAaQBjACAAZABhAHQAYQAgAHAAYQByAHQAaQB0AGkAbwBuAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAApLuU3tEGQE2har/VAXnWrJLkWbwPspVJsUiN7QMMfsIA
QPgaAAAAAP8/8hsAAAAAAQAAAAAAAIBCAGEAcwBpAGMAIABkAGEAdABhACAAcABhAHIAdABpAHQA
aQBvAG4AAACnCvx/AABwUYZLqAIAAMCR3EuoAgAAvzp1gHZFAAAEAAAAAwAAgAEAAAALAOx4sJ/B
n5dxF3QT6KvwJGhxnld9pkGqElMS3Ie1+jRosAAAABiAj1cAAAAAOH0WAAAAAAAAAAAQAAAAJAA
AAAAAAAAgEMANBBAwoAAAAAAQEGAAURAxIKAAAA//8AAAQBKgACAAAAAKgPAAAAAAAAIAMAAAAA
ADxip4weBKtPjBL0moa4XXMCAgQERgBcAEUARgBJAFwATQBpAGMAcgBvAHMAbwBmAHQAXABCAG8A
bwB0AFwAYgBvAG8AdABtAGcAZgB3AC4AZQBmAGkAAAB//wQABAAAAAMAAIABAAAACwCVM99MXLEN
ElINW9ucHV1i5vuARdfVeQyMMnsFLsYKNUwAAAAYoKBXAAAAAACtAgAAAAAAAAAAAAAAAAAsAAAA
AAAAAAQHFAA1e7vNM2jWTpqyV9Ks3fbwBAYUACGqLEYUdgNFg26KtvRmIzF//wQABAAAAAcAAIAB

AAAACwBwRPBjA+VPqWw/zRoPEQR8A9IJB0Rwsf1gRgyfAH4opi8AAABSZXR1cm5pbmcgZnJvbSBF
RkkgQXBwbGljYXRpb24gZnJvbSBCb290IE9wdGlvbgQAAAAHAACAAQAAAAsAPWdytPhO1HWV1yos
TF/9FfW7csdQf+JvKq7ixp1WM7ooAAAAQ2FsbGluZyBFRkkgQXBwbGljYXRpb24gZnJvbSBCb290
IE9wdGlvbgEAAAAJAACAAQAAAAsANmbRbDDrxGyjLHxuMiIXWqFQgd2dJLZJM80z92TMmrkgAAAA
AQAAAAAAAABEFf3ylJcsSpku5bvPIOOUAABnYwAAAAAEAAAAAwAAgAEAAAALAMuJFKnSmpw1AZzW
dr0s8uBd+Y0kjJkEuf4ClWNyyMF7TAAAABiweFcAAAAAgI4OAAAAAAAAAAAAAAAAAACwAAAAAAAA
BAcUADV7u80zaNZOmrJX0qzd9vAEBhQAg6UEfD6eHE+tZeBSaNC00X//BAAEAAAAAwAAgAEAAAAL
ANdidGjWJsOi67Wddm9Skj8qo2ec2pBP/f5Xe8VwxVb2jAAAABjgrFgAAAAAQEgAAAAAAAAAAAA
AAAAAGwAAAAAAAAAgEMANBBAwoAAAAAAQEGAAAUAwUGAAMABAEqAAEAAAA/AAAAAAAAAMG/7gAA
AAAAgXcmFAAAAAAAAAAAAAAAAAEBBAQmAFwAVABjAGcAMgBEAHUAbQBwAEwAbwBnAC4AZQBmAGkA
AAB//wQABAAAAAMAAIABAAAACwDXYnRo1ibDouu1nXZvUpI/KqNnnNqQT/3+V3vFcMVW9owAAAAY
4KxYAAAAAEBIAAAAAAAAAAAAAAAAAAABsAAAAAAAAAAIBDADQQQMKAAAAAAEBBgAAFAMFBgADAAQB
KgABAAAAPwAAAAAAADBv+4AAAAAAIF3JhQAAAAAAAAAAAAAAAABAQQEJgBcAFQAYwBnADIARAB1
AG0AcABMAG8AZwAuAGUAZgBpAAAAf/8EAAQAAAADAACAAQAAAAsAHoNEmRcfb3nkbytX/Ka07v6c
gnjmuHKAHz/oo4m8IfKMAAAAGECsWAAAAADASAAAAAAAAAAAAAAAAAAAbAAAAAAAAAACAQwA0EED
CgAAAAABAQYAABQDBQYAAwAEASoAAQAAAD8AAAAAAAAAwb/uAAAAAACBdyYUAAAAAAAAAAAAAAAA
AQEEBCYAXABUAGMAZwAyAEQAdQBtAHAATABvAGcALgBlAGYAaQAAAH//BAAEAAAAAwAAgAEAAAAL
AEVCUwWb3a2APmgw4kTl5sbkiucgGtoxngRvb1IRkmrtjAAAABgwrFgAAAAwEkAAAAAAAAAAAAA
AAAAAGwAAAAAAAAAgEMANBBAwoAAAAAAQEGAAAUAwUGAAMABAEqAAEAAAA/AAAAAAAAAMG/7gAA
AAAAgXcmFAAAAAAAAAAAAAAAAAEBBAQmAFwAVABjAGcAMgBEAHUAbQBwAEwAbwBnAC4AZQBmAGkA
AAB//wQABAAAAAMAAIABAAAACwCU8j6epKtWZUF/Xc9g1MZsxsAO7vxVKp0Sohufc/+PdowAAAAY
4KtYAAAAAEBJAAAAAAAAAAAAAAAAAAABsAAAAAAAAAAIBDADQQQMKAAAAAAEBBgAAFAMFBgADAAQB
KgABAAAAPwAAAAAAADBv+4AAAAAAIF3JhQAAAAAAAAAAAAAAAABAQQEJgBcAFQAYwBnADIARAB1
AG0AcABMAG8AZwAuAGUAZgBpAAAAf/8EAAQAAAADAACAAQAAAAsA5dAldlVqUXqdhPlKUHBknL9q
h+RBSh4vf5JMZR5F0COMAAAAGOCrWAAAAABASQAAAAAAAAAAAAAAAAAAbAAAAAAAAAACAQwA0EED
CgAAAAABAQYAABQDBQYAAwAEASoAAQAAAD8AAAAAAAAAwb/uAAAAAACBdyYUAAAAAAAAAAAAAAAA
AQEEBCYAXABUAGMAZwAyAEQAdQBtAHAATABvAGcALgBlAGYAaQAAAH//BAAEAAAAAwAAgAEAAAAL
AKuA719q+kVmuiNIIC6KW/mWgZkrgdoqrEN72lRoS1d9jAAAABjgq1gAAAAA4EwAAAAAAAAAAAA
AAAAAGwAAAAAAAAAgEMANBBAwoAAAAAAQEGAAAUAwUGAAMABAEqAAEAAAA/AAAAAAAAAMG/7gAA
AAAAgXcmFAAAAAAAAAAAAAAAAAEBBAQmAFwAVABjAGcAMgBEAHUAbQBwAEwAbwBnAC4AZQBmAGkA
AAB//wQABAAAAAMAAIABAAAACwCO5+91NXgnmqXqUpfPMyMCa7EFpcZDgWe3ZmUsxi0pwowAAAAY
sKtYAAAAAGBMAAAAAAAAAAAAAAAAAAABsAAAAAAAAAAIBDADQQQMKAAAAAAEBBgAAFAMFBgADAAQB
KgABAAAAPwAAAAAAADBv+4AAAAAAIF3JhQAAAAAAAAAAAAAAAABAQQEJgBcAFQAYwBnADIARAB1
AG0AcABMAG8AZwAuAGUAZgBpAAAAf/8EAA==

PC Client RIM:

<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<SoftwareIdentity xmlns="http://standards.iso.org/iso/19770/-2/2015/schema.xsd"
xmlns:ns2="http://www.w3.org/2000/09/xmldsig#" corpus="false" name="Example.com BIOS" patch="false"
supplemental="false" tagId="94f6b457-9ac9-4d35-9b3f-78804173b65as" tagVersion="0" version="01"
versionScheme="multipartnumeric" xml:lang="en">
  <Entity name="Example Inc" regid="http://Example.com" role="softwareCreator tagCreator"/>
  <Link href="https://Example.com/support/ProductA/firmware/installfiles" rel="installationmedia"/>
  <Meta xmlns:n8060="http://csrc.nist.gov/ns/swid/2015-extensions/1.0"
xmlns:rim="https://trustedcomputinggroup.org/wp-content/uploads/TCG_RIM_Model"
n8060:colloquialVersion="Firmware_2019" n8060:edition="IOT" n8060:product="ProductA" n8060:revision="r2"
rim:bindingSpec="PC Client RIM" rim:bindingSpecVersion="1.2"
rim:pcURIGlobal="https://Example.com/support/ProductA/firmware/rims" rim:platformManufacturerId="00213022"
rim:platformManufacturerStr="BIOSVendorA" rim:platformModel="A0" rim:platformVersion="12"
rim:rimLinkHash="88f21d8e44d4271149297404df91caf207130bfa116582408abd04ede6db7f51"/>
  <Payload>
    <Directory name="rim">
      <File xmlns:SHA256="http://www.w3.org/2001/04/xmlenc#sha256"
SHA256:hash="4479ca722623f8c47b703996ced3cbd981b06b1ae8a897db70137e0b7c546848"
name="Example.com.iotBase.bin" size="7549"/>
    </Directory>
  </Payload>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
      <Reference URI="">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
        <DigestValue>fze9UG1Ft9l80Yn8Z4oDTy7G0iCtk+y7hIfoOru6pDI=</DigestValue>
      </Reference>
    </SignedInfo>

<SignatureValue>b21c8nvkjYO0MZvm8quOlLkd/ocTrdpQ55G7mKELy4wDHRxKe3LLdKXOFpab9A9oTwtdEXZnH
TCahwdt31YALMuTSY4kBORuPDsaby/Cte/35/2gGwkZEEE1DNBVXAG97SiuBd5koebcT8TTdGGis6wr
UzcDnFXEt3LLAU8ZHhl7weqeyuqsNP12teCpb2Ru9FDWBOUjgOeBo7P6qdJJCG3txmsD1pjA92zg
zuLzwiY1B+sPk8aC5n9LiXOgaDr2MLuijmIrGJzOYEItgMQ+a5ncyZtb8hHdC93xnk0IlnaG5wuv
1Ribeg/Zr6z5k4Yg6Z+ErOPqlDSyPJMZEJZdkQ==</SignatureValue>
    <KeyInfo>
      <KeyName>2fdeb8e7d030a2209daa01861a964fedecf2bcc1</KeyName>
      <KeyValue>
        <RSAKeyValue>

<Modulus>p3WVYaRJG7EABjbAdqDYZXFSTV1nHY9Ol9A5+W8t5xwBXBryZCGWxERGr5AryKWPxd+qzjj+cFpx

xkM6N18jEhQIx/CEZePEJqpluBO5w2wTEOe7hqtMatqgDDMeDRxUuIpP8LGP00vh1wyDFFew90d9
dvT3bcLvFh3a3ap9bTm6aBqPup5CXpzrwIU2wZfgkDytYVBm+8bHkMaUrgpNyM+5BAg2zl/Fqw0q
otjaGr7PzbH+urCvaGbKLMPoWkVLIgAE8Qw98HTfoYSFHC7VYQySrzIinaOBFSgViR72kHemH2lW
jDQeHiY0VIoPik/jVVIpjWe6zzeZ2S66Q/LmjQ==</Modulus>
        <Exponent>AQAB</Exponent>
      </RSAKeyValue>
    </KeyValue>
    <X509Data>
      <X509SubjectName>CN=example.RIM.signer,OU=PCClient,O=Example,ST=VA,C=US</X509SubjectName>

<X509Certificate>MIIDoTCCAomgAwIBAgIJAPB+r6VBhBn5MA0GCSqGSIb3DQEBCwUAMFMxCzAJBgNVBAYTAl
VTMQsw
CQYDVQQIDAJWQTEQMA4GA1UECgwHRXhhbXBsZTERMA8GA1UECwwIUENDbGllbnQxEjAQBgNVBAMM
CUV4YW1wbGVDQTAeFw0yMDAzMTExODExMjJaFw0zMDAxMTgxODExMjJaMFwxCzAJBgNVBAYTAlVT
MQswCQYDVQQIDAJWQTEQMA4GA1UECgwHRXhhbXBsZTERMA8GA1UECwwIUENDbGllbnQxGzAZBgNV
BAMMEmV4YW1wbGUuUklNLnNpZ25lcjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKd1
lWGkSRuxAAY2wHag2GVxUk1dZx2PTpfQOflvLeccAVwa8mQhlsRERq+QK8ilj8Xfqs44/nBaccZD
OjdfIxIUCMfwhGXjxCaqZbgTucNsExDnu4arTGraoAwzHg0cVLiKT/Cxj9NL4dcMgxRXsPdHfXb0
923C7xYd2t2qfW05umgaj7qeQl6c68CFNsGX4JA8rWFQZvvGx5DGlK4KTcjPuQQINs5fxasNKqLY
2hq+z82x/rqwr2hmyizD6FpFSyIABPEMPfB036GEhRwu1WEMkq8yIp2jgRUoFYke9pB3ph9pVow0
Hh4mNFSKD4pP41VSKY1nus83mdkuukPy5o0CAwEAAaNvMG0wHQYDVR0OBBYEFC/euOfQMKIgnaoB
hhqWT+3s8rzBMB8GA1UdIwQYMBaAFEahuO3bpnFf0NLneoo8XW6aw5Y4MAkGA1UdEwQCMAAwCwYD
VR0PBAQDAgbAMBMGA1UdJQQMMAoGCCsGAQUFBwMDMA0GCSqGSIb3DQEBCwUAA4IBAQBl2Bu9xpnH
CCeeebjx+ILQXJXBd6q5+NQlV3zzBrf0bleZRtsOmsuFvWQoKQxsfZuk7QcSvVd/1v8mqwJ0PwbF
KQmrhIPWP+iowiBNqpG5PH9YxhpHQ1osOfibNLOXMhudIQRY0yAgqQf+MOlXYa0stX8gkgftVBDR
utuMKyOTf4a6d8TUcbG2RnyzO/6S9bq4cPDYLqWRBM+aGN8e00UWTKpBl6/1EU8wkJA6WdllK2e8
mVkXUPWYyHTZ0qQnrYiuLr36ycAznABDzEAoj4tMZbjIAfuscty6GgzxI1WbyZLI6YzyXALwaYvr
crTLeyFynlKxuCfDnr1SAHDM65BY</X509Certificate>
    </X509Data>
  </KeyInfo>
 </Signature>
</SoftwareIdentity>

Appendix E: RIM Guidance for OS developers

Operating systems that manage the TPM's PCRs 8-15 need to provide RIM Bundles during OS installation and updates to those PCR values that change when OS updates are distributed. RIM Bundle distribution can be accommodated by the OS packaging or installation/update services by including a RIM Bundle to be installed on the EFI partition.

An Operating system that manages the TPM's PCRs 8-15 should provide PC Client RIM Bundles and include the instance in any OS installation or update process that effects any of the PCR values. This is potentially operationally infeasible, depending on how the OS loads and measures drivers (in parallel).

The OS RIM should follow the requirements for Supplemental RIMs as defined in section 4.2.1.

The Event Log Assertions file should exclude any PCR's not measured into by the OS.

For the TPM PCR Log Assertions the TPML_PCR_SELECTION (as defined in the Trusted Platform Module Library Part 3 [19]) should be set to contain only PCRs 8-15 that are applicable to the OS.

Most operating systems provide package management subsystems that utilize publicly accessible mirrors to assist in the installation and update processes. These systems should provide RIM Bundles that are specific to the device configuration.

Any packaging of Firmware updates (e.g. rpm, deb, msi, etc.) should include the associated RIM Bundle. Any installation/update of OS packages that include firmware updates should include placement of the RIM Bundle in accordance with the EFI System Partition Storage section. The definition of the packaging is out of scope for this specification.

Appendix F: References

[1] Trusted Computing Group, “Trusted Attestation Protocol (TAP) Information Model for TPM Families 1.2 and 2.0 and DICE Family 1.0”, https://trustedcomputinggroup.org/wp-content/uploads/TNC_TAP_Information_Model_v1.00_r0.29A_publicreview.pdf

[2] IEFT RFC-2119, "Key words for use in RFCs to Indicate Requirement Levels", https://tools.ietf.org/html/rfc2119

[3] NISTIR-8660, “Guidelines for the Creation of Interoperable Software ID (SWID) Tags”, April 2016, https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8060.pdf

[4] ISO/IEC 19770-2:2015 International Organization for Standardization/International Electrotechnical Commission, Information technology -- Software asset management -- Part 2: Software identification tag, ISO/IEC 19770-2:2009, November 2009. http://www.iso.org/iso/catalogue_detail?csnumber=65666

[5] TCG TPM 2.0 Provisioning Guidance, March 2017, https://trustedcomputinggroup.org/wp-content/uploads/TCG-TPM-v2.0-Provisioning-Guidance-Published-v1r1.pdf

[6] TCG Infrastructure Working Group Reference Manifest (RM) Schema Specification, November 2006, https://trustedcomputinggroup.org/wp-content/uploads/IWG-Reference_Manifest_Schema_Specification_v1.pdf

[7] TCG PC Client Platform Firmware Profile, October 2018, https://trustedcomputinggroup.org/wp-content/uploads/TCG_PCClient_Specific_Platform_Profile_for_TPM_2p0_1p04_PUBLIC.pdf

[8] XML Signature Syntax and Processing Version 2.0, W3C Working Group Note 23 July 2015, http://www.w3.org/TR/xmldsig-core2/

[9] TCG TSS2.0 Overview and Common Structures Specification, Version 0.90 Revision 03 January 4,2018, https://trustedcomputinggroup.org/wp-content/uploads/TSS_Overview_Common_Structures_Version-0.9_Revision-03_Review_030918.pdf

[10] TCG Platform Certificate Profile, Version 1.1 Revision 1 5 13 Feb 2019, https://trustedcomputinggroup.org/wp-content/uploads/IWG_Platform_Certificate_Profile_v1p1_r15_pubrev.pdf

[11] TCG PC Client Platform Firmware Integrity Measurement (FIM) specification, Version1 Revision 24, https://trustedcomputinggroup.org/wp-content/uploads/TCG_PC_Client-FIM_v1r24_3feb20.pdf

[12] TCG Reference Integrity Manifest Information Model, https://trustedcomputinggroup.org/wp-content/uploads/TCG_RIM_Model_v1-r13_2feb20.pdf

[13] IETF RFC-4122 , “A Universally Unique IDentifier (UUID) URN Namespace”, https://tools.ietf.org/html/rfc4122

[15] IANA Private Enterprise Numbers, http://www.iana.org/assignments/enterprise-numbers/enterprise-numbers

[16] TCG Algorithm Registry,Family “2.0", Level 00 Revision 01.22,February 9, 2015,https://trustedcomputinggroup.org/wp-content/uploads/TCG_Algorithm_Registry_Rev_1.22.pdf

[17] NIST, The SWID Tag Validation (SWIDVal) Tool Version 0.5.0, https://csrc.nist.gov/CSRC/media/Projects/Software-Identification-SWID/tools/swidval-0.5.0-swidval.zip

[18] NIST SWID Tag extensions from NIST IR 8060, https://csrc.nist.gov/schema/swid/2015-extensions/swid-2015-extensions-1.0.xsd

[19] Trusted Platform Module Library Part 3: Commands, Family “2.0” Level 00 Revision 01.38 September 29, 2016 https://www.trustedcomputinggroup.org/wp-content/uploads/TPM-Rev-2.0-Part-3-Commands-01.38.pdf

[20] X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, RFC 6960, https://tools.ietf.org/html/rfc6960

[21] FOUNDATIONAL TRUST FOR IOT AND RESOURCE CONSTRAINED DEVICES https://trustedcomputinggroup.org/work-groups/dice-architectures/

[22] Trusted Platform Module (TPM) https://trustedcomputinggroup.org/work-groups/trusted-platform-module/

[23] Integrity Measurement Architecture, https://sourceforge.net/p/linux-ima/wiki/Home/

[24] RFC 4122 A Universally Unique IDentifier (UUID) URN Namespace, https://tools.ietf.org/html/rfc4122

